DECENTRALIZED COMMERCE – A PRIMER ON WHY DECENTRALIZED REPUTATION VERIFICATION SYSTEMS ARE NEEDED

Wulf A. Kaal**

Abstract

Decentralized reputation verification systems enable mathematically rigid smart contracts to become more adjustable for the needs of business. Code is law principles can be upheld for smart contracts when reputation verification enables smart contract template verification. Validated templates of smart contracts increase trust for counterparties. The validation removes the need for costly back-testing and facilitates decentralized business transactions at unprecedented scale.

***Key Words**:* Decentralized Commerce, Reputation Verification, Emerging Technology, Crypto Economics, Token Models, Incentive Design, Velocity, Supply, Demand, Tokens, Blockchain, Distributed Ledger Technology

***JEL Categories**:* K20, K23, K32, L43, L5, O31, O32

** Professor of Law, *University of St. Thomas School of Law (Minneapolis, USA)*

Table of Contents

I. Introduction

Decentralized commerce may generically be defined as the global exchange of financial instruments, goods and services via decentralized and emerging technologies. Starting with the emergence of the Bitcoin protocol in 2009, the digital asset market is a market for investment opportunities in virtual assets. Stock is not inherently digital as it has strong ties to the real world. By contrast, Bitcoin is a purely digital asset because it only exists in the virtual world. Narrowly construed, digital assets are instantiated through computer code and depend on so-called "consensus computer algorithms" to trigger and validate a transaction in a given digital asset. Broadly construed, digital assets can include video games in the broadest sense and items sold in video games can be digital assets without a consensus algorithm that validates the transaction or provides a level of security.

Smart contracts allow anonymous parties to engage in decentralized commerce by providing automated contracting that self-executes and self-regulates according to mathematical strictures. Smart contracts are evolving quickly. Their evolution enables most business logic to be included in smart contracts over time.

II. Example

A simple example involving smart property may help illustrate the uses of smart contracting. The example illustrates that smart contracts can self-execute in a decentralized environment with anonymous actors.

Consider the example of a home owner making her house available for rent. The home owner posts a smart contract with the terms she will accept, including length of stay, price per night etc. After encumbering digital currency in the smart contract, a renter would be able to unlock and use the house with a private key digital signature which would only work for the contractually agreed period paid. The smart lock of the house allows the renter to enter if and when all conditions specified in the contract have been satisfied, e.g. the deposit was encumbered and other qualifying criteria for the renter were fulfilled. On the one hand, if the home is not in the agreed upon condition at any time the rental contract started, the smart contract could automatically reimburse (part of) the encumbered deposit. In turn, if the house was not returned at the agreed upon time, the renter would lose (part of) the encumbered deposit.

III. Benefits of Smart Contracts

Smart contracts provide multiple benefits for businesses. Smart contracts are intended to simplify and automate business, removing transaction costs and creating certainty for counterparties. They make business transactions fully secure and efficient. It is also inexpensive to run smart contracts on a blockchain. The smart

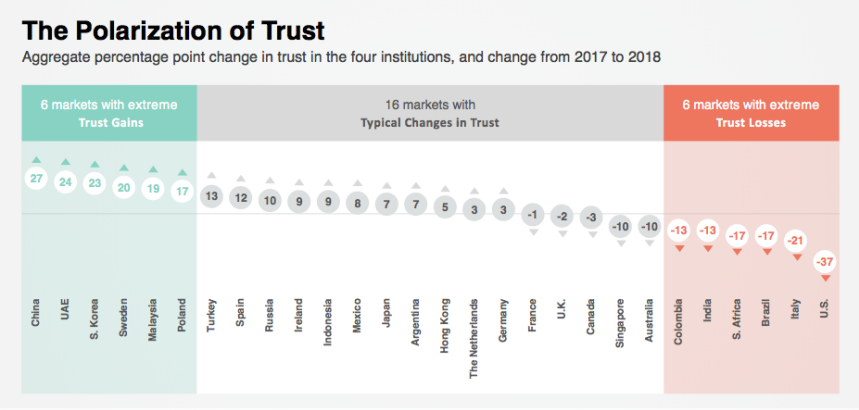
contract near optimally coordinates the relationship between the anonymous parties and removes the need for agency / intermediaries almost entirely. Negotiation between counterparties is near minimal, transaction cost typically associated with contracting are almost entirely removed by the automation. The inherent mathematical logic of computerized code in smart contracts can optimally clarify parties' intent. It also increases certainty and creates unparalleled efficiency which in turn incentivizes commerce. Most importantly, the smart contract removes centralized guarantors. The smart contract self-regulates. Only limited legal recourse is available if something goes wrong in the execution of the terms of the contract.

IV. Downsides of Smart Contracts

Despite the significant benefits of smart contracting for business and society, smart contracts are subject to significant limitations. Human business interactions require a flexibility that is at odds with merciless mathematical logic of smart contracts. Human interaction requires flexibility in interpreting intent that cannot be ensured by smart contracting because smart contract code does not follow the same logic on similar terms as natural human language. Smart contracts also undermine counterparties' ability to continue collaboration when unanticipated eventualities arise. In most cases of unfulfilled parameters, the smart contract will simply cancel out. Human business interaction also typically requires the possibility that each party may fulfill only a portion of any intended collaboration. While more sophisticated smart contracts over time can fulfil some of these human business requirements, the needed

flexibility in existing decentralized protocols will unlikely ever be attained unless a decentralized verification system is built into decentralized commerce.

V. Trust Problem



Source: 2018 Edelman Trust Barometer. Trust Volatility Measure. The net year-over-year (2017-2018) percentage point change across the four institutions (TRU_INS). General population, 28-market global total. For more details on how the Trust Volatility Measure was calculated, please refer to the Technical Appendix.

Trust barometers, such as the Edelman report, assessing the level of trust in centralized institutions suggests radical depreciation in trust between the years 2017 and 2018. While smart contracting in decentralized system can be perceived as creating trust through mathematical and coded—preordained coordination without agency problems, several factors suggest that decentralized commerce via decentralized solutions is equally afflicted with trust issues.

Trust between counterparties in decentralized systems can only limitedly be assured by smart contracts. In our example above, the tenant of the smart property cannot fully know if the landlord is providing a worthy property. In turn, the landlord cannot know in advance how likely the tenant will destroy the premises. Moreover, neither party to the contract can trust the programmed parameters of

the smart entirely. In simpler smart contracts such trust may be more justified if the smart contract template has a history of successful executions. In more complex smart contracts, however, the programmed logic may not execute. In other words, in more complex smart contracts, the counterparties to the contract cannot fully know if the contract will do what it was programmed to do and whether it will have bugs or otherwise follow another logic that was not anticipated by the parties to the contract. Even small and simple smart contracts often have bugs that trigger unforeseeable consequences.

VI. Decentralized Reputation as the Solution

To solve the issues of trust in decentralized commerce, an intangible value system is needed. The transferability of stores of value entailed in cryptocurrencies creates core points of attack and undermines the very nature of decentralization. Because of the store of value entailed in cryptocurrencies (and really any currencies or store of value), exercise of power over such value inevitably leads to centralization due to economies of scale.

Reputation as a metric and store of value does not suffer the same consequences and does not lead to centralization because it must be earned, it can be lost, yet it cannot be turned into a fungible store of value that allows the exchange for goods etc. Hence, unlike currencies, reputation does not naturally lead to centralization.

In as much as reputation enables truly decentralized solutions reputation is also the key ingredient that enables commerce. Centralized capitalist institutions have been built entirely around centralized and hierarchical reputation systems. Bitcoin proved that a decentralized system can automate the transfer of valuable digital currency without intermediaries, no centralized authority for recourse, efficiently, securely, cheaply, and expeditiously. Until blockchain technology was introduced via bitcoin in 2009, decentralized reputation system mostly relied on the old and corruptible concept of the Web of Trust.

Decentralized reputation verification systems enable mathematically rigid smart contracts to become more adjustable for the needs of business. Reputation verification becomes the backstop for smart contracting. While the rigorous standard of "code is law", associated with smart contracting, can be upheld, reputation verification enables smart contract template verification. Validated templates of smart contracts increase trust for counterparties. The validation removes the need for costly back-testing and experimentation with smart contract templates.

To truly increase trust for counterparties in decentralized smart contract-based commerce, counterparties need to be able to review a long history of each other's conduct in decentralized commerce and the history of performance in earlier smart contracts. This is possible through a platform that creates reputation for both parties and for the smart contract itself. Similar business deals and contracts

between counterparties need to be organized and reviewable by the public. The history of transactions has to be fully openly viewable and verifiable, so that business parties can see that their counterparties will perform as expected. This necessitates that counterparties' actions in decentralized commerce endure and become part of a public record. In other words, counterparties' actions need to stick. Their actions have to become part of a precedence system that is meaningful.